

# TRUNCATION OF HAAR RANDOM MATRICES IN $\mathrm{GL}_N(\mathbb{Z}_m)$

YANQI QIU

**ABSTRACT.** The asymptotic law of the truncated  $S \times S$  random submatrix of a Haar random matrix in  $\mathrm{GL}_N(\mathbb{Z}_m)$  as  $N$  goes to infinity is obtained. The same result is also obtained when  $\mathbb{Z}_m$  is replaced by any commutative compact local ring whose maximal ideal is topologically closed.

## 1. INTRODUCTION

In the theory of random matrices, some particular attentions are paid recently to the asymptotic distributions of those truncated  $S \times S$  upper-left corner of a large  $N \times N$  random matrices from different matrix ensembles (CUE, COE, Haar Unitary Ensembles, Haar Orthogonal Ensembles), see [6, 4, 2, 1].

In the present paper, we consider the truncation of a Haar random matrix in  $\mathrm{GL}_N(\mathbb{Z}_m)$  with  $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ . This research is motivated by its application in a forthcoming paper on the classification of ergodic measures on the space of infinite  $p$ -adic matrices, where the asymptotic law of a fixed size truncation of the Haar random matrix from the group of  $N \times N$  invertible matrices over the ring of  $p$ -adic integers is essentially used and is derived from a particular case of our main result, Theorem 3.1. Remark that the ring of  $p$ -adic integers is isomorphic to the inverse limit of the rings  $\mathbb{Z}_{p^n}$ .

## 2. NOTATION

Fix a positive integer  $m \in \mathbb{N}$ . Consider the ring  $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ . Let  $\mathbb{Z}_m^\times$  be the multiplicative group of invertible elements of the ring  $\mathbb{Z}_m$ . For any  $N \in \mathbb{N}$ , denote by  $M_N(\mathbb{Z}_m)$  the matrix ring over  $\mathbb{Z}_m$  and denote by  $\mathrm{GL}_N(\mathbb{Z}_m)$  the finite group of  $N \times N$  invertible matrices over  $\mathbb{Z}_m$ .

---

*Date:* February 29, 2016.

2010 *Mathematics Subject Classification.* Primary 60B20; Secondary 15B33, 60B10.

*Key words and phrases.* Random matrix, invertible matrix, commutative compact local ring, truncation, asymptotic law.

This work is supported by the grant IDEX UNITI - ANR-11-IDEX-0002-02, financed by Programme “Investissements d’Avenir” of the Government of the French Republic managed by the French National Research Agency.

Note that we have

$$\mathrm{GL}_N(\mathbb{Z}_m) = \left\{ A \in M_N(\mathbb{Z}_m) \mid \det A \in \mathbb{Z}_m^\times \right\}.$$

Let  $\mathcal{U}_N(m)$  denote the uniform distribution on  $M_N(\mathbb{Z}_m)$  and let  $\mu_N(m)$  denote the uniform distribution on  $\mathrm{GL}_N(\mathbb{Z}_m)$ . Note that  $\mu_N(m)$  is the normalized Haar measure of the group  $\mathrm{GL}_N(\mathbb{Z}_m)$ .

The cardinality of any finite set  $E$  is denoted by  $|E|$ .

### 3. MAIN RESULT

Fix a positive integer  $S \in \mathbb{N}$ . If  $X$  is a  $N \times N$  matrix (in what follows, the range of the coefficients of  $X$  can vary), then we denote by  $X[S]$  the truncated upper-left  $S \times S$  corner of  $X$ , i.e.,

$$(3.1) \quad X[S] := (X_{ij})_{1 \leq i, j \leq S}$$

Let  $X^{(N)}(m)$  be a random matrix sampled with respect to the normalized Haar measure of  $\mathrm{GL}_N(\mathbb{Z}_m)$ , that is, the probability distribution  $\mathcal{L}(X^{(N)}(m))$  of the random matrix  $X^{(N)}(m)$  satisfies

$$\mathcal{L}(X^{(N)}(m)) = \mu_N(m).$$

By adapting the notation (3.1), we denote by  $X^{(N)}(m)[S]$  the truncated upper-left  $S \times S$  corner of the random matrix  $X^{(N)}(m)$ , i.e.,

$$X^{(N)}(m)[S] := \left( X^{(N)}(m)_{ij} \right)_{1 \leq i, j \leq S}$$

**Theorem 3.1.** *The probability distribution  $\mathcal{L}(X^{(N)}(m)[S])$  of the truncated random matrix  $X^{(N)}(m)[S]$  converges weakly, as  $N$  tends to infinity, to the uniform distribution  $\mathcal{U}_S(m)$  on  $M_S(\mathbb{Z}_m)$ .*

For any positive integer  $u \in \mathbb{N}$ , we write  $Q_u : \mathbb{Z} \rightarrow \mathbb{Z}_u = \mathbb{Z}/u\mathbb{Z}$  the quotient map. If  $v$  is another positive integer such that  $u$  divides  $v$ , then since  $v\mathbb{Z} \subset u\mathbb{Z} = \ker(Q_u)$ , the map  $Q_u$  induces in a unique way a map  $Q_u^v : \mathbb{Z}_v \rightarrow \mathbb{Z}_u$ . Note that the map  $Q_u^v : \mathbb{Z}_v \rightarrow \mathbb{Z}_u$  is surjective and

$$(3.2) \quad \left| (Q_u^v)^{-1}(x) \right| = \frac{v}{u}, \forall x \in \mathbb{Z}_u,$$

that is, for each element  $x \in \mathbb{Z}_u$ , the cardinality of the pre-image of  $x$  is  $v/u$ .

By slightly abusing the notation, for any matrix  $A = (a_{ij})_{1 \leq i, j \leq N}$  in  $M_N(\mathbb{Z})$ , we set

$$Q_u(A) := (Q_u(a_{ij}))_{1 \leq i, j \leq N}.$$

Similarly, for any matrix  $B = (b_{ij})_{1 \leq i, j \leq N}$  in  $M_N(\mathbb{Z}_v)$ , we set

$$Q_u^v(B) := (Q_u^v(b_{ij}))_{1 \leq i, j \leq N}.$$

By the prime factorization theorem, we may write in a unique way

$$(3.3) \quad m = p_1^{r_1} \cdots p_s^{r_s},$$

where  $p_1, \dots, p_s$  are distinct prime numbers and  $r_1, \dots, r_s$  are positive integers. By the Chinese remainder theorem, we have an isomorphism of the following two rings:

$$(3.4) \quad \mathbb{Z}_m \simeq \mathbb{Z}_{p_1^{r_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{r_s}}.$$

A natural isomorphism is provided by the map  $\phi : \mathbb{Z}_m \longrightarrow \mathbb{Z}_{p_1^{r_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{r_s}}$  defined by

$$(3.5) \quad \phi(x) = (Q_{p_1^{r_1}}^m(x), \dots, Q_{p_s^{r_s}}^m(x)) \quad (\forall x \in \mathbb{Z}_m).$$

*Simple case:* Let us first assume that in the factorization (3.3), we have  $s = 1$ . For simplifying the notation, let us write  $m = p^r$ .

Writing  $\mathbb{F}_p$  for the finite field  $\mathbb{Z}/p\mathbb{Z}$ . We have the following characterization of  $\text{GL}_N(\mathbb{Z}_{p^r})$ .

**Theorem 3.2** ([3, Theorem 3.6]). *A matrix  $M$  is in  $\text{GL}_N(\mathbb{Z}_{p^r})$  if and only if  $Q_p^{p^r}(M) \in \text{GL}_N(\mathbb{F}_p)$ .*

Given a matrix  $W \in M_S(\mathbb{Z}_{p^r})$  such that  $Q_p^{p^r}(W) \in \text{GL}_S(\mathbb{F}_p)$ , then a moment of thinking allows us to write

$$(3.6) \quad \left| \{X \in \text{GL}_N(\mathbb{F}_p) : X(S) = Q_p^{p^r}(W)\} \right| = p^{S(N-S)} \cdot \prod_{j=0}^{N-S-1} (p^N - p^{S+j}),$$

where  $p^{S(N-S)}$  the number of choices of  $(X_{ij})_{1 \leq i \leq S, S+1 \leq j \leq N}$  with coefficients in  $\mathbb{F}_p$  and  $\prod_{j=0}^{N-S-1} (p^N - p^{S+j})$  is the number of choices of  $(X_{ij})_{S+1 \leq i \leq N, 1 \leq j \leq N}$ .

It follows that, for any matrix  $W \in M_S(\mathbb{Z}_{p^r})$ , we have

$$(3.7) \quad \left| \{X \in \text{GL}_N(\mathbb{F}_p) : X(S) = Q_p^{p^r}(W)\} \right| \leq p^{S(N-S)} \prod_{j=0}^{N-S-1} (p^N - p^{S+j}).$$

We also have for any matrix  $W \in M_S(\mathbb{Z}_{p^r})$ ,

$$(3.8) \quad \left| \{X \in \text{GL}_N(\mathbb{F}_p) : X(S) = Q_p^{p^r}(W)\} \right| \geq \prod_{i=0}^{S-1} (p^{N-S} - p^i) \prod_{j=0}^{N-S-1} (p^N - p^{S+j}),$$

where  $\prod_{i=0}^{S-1} (p^{N-S} - p^i)$  is the number of choices of  $(X_{ij})_{1 \leq i \leq S, S+1 \leq j \leq N}$  with coefficients in  $\mathbb{F}_p$  such that

$$\text{rank} \left[ (X_{ij})_{1 \leq i \leq S, S+1 \leq j \leq N} \right] = S.$$

Recall that  $X^{(N)}(m)$  is a random matrix sampled with respect to the Haar measure of  $\text{GL}_N(\mathbb{Z}_m) = \text{GL}_N(\mathbb{Z}_{p^r})$ . By combining (3.2), (3.7)

and (3.8), we see that the cardinality

$$n_N(W) := \left| \{X \in \mathrm{GL}_N(\mathbb{Z}_{p^r}) : X(S) = W\} \right|$$

satisfies the relation

$$\begin{aligned} p^{r-1} \prod_{i=0}^{S-1} (p^{N-S} - p^i) \prod_{j=0}^{N-S-1} (p^N - p^{S+j}) &\leq n_N(W) \\ &\leq p^{r-1} p^{S(N-S)} \prod_{j=0}^{N-S-1} (p^N - p^{S+j}). \end{aligned}$$

As a consequence, for any  $W_1, W_2 \in M_S(\mathbb{Z}_{p^r})$ , the following relation holds:

$$(3.9) \quad \frac{\prod_{i=0}^{S-1} (p^{N-S} - p^i)}{p^{S(N-S)}} \leq \frac{\mathbb{P}(X^{(N)}(m)[S] = W_1)}{\mathbb{P}(X^{(N)}(m)[S] = W_1)} \leq \frac{p^{S(N-S)}}{\prod_{i=0}^{S-1} (p^{N-S} - p^i)}.$$

Hence we get

$$(3.10) \quad \lim_{N \rightarrow \infty} \frac{\mathbb{P}(X^{(N)}(m)[S] = W_1)}{\mathbb{P}(X^{(N)}(m)[S] = W_1)} = 1.$$

Since the set  $M_S(\mathbb{Z}_m)$  is finite, the above equality (3.10) implies that  $\mathcal{L}(X^{(N)}(m)[S])$  converges weakly, as  $N$  tends to infinity, to the uniform distribution  $\mathcal{U}_S(m)$  on  $M_S(\mathbb{Z}_m)$ .

*General case:* It is clear that, for any  $N \in \mathbb{N}$ , the isomorphism  $\phi$  defined in (3.5) induces in a natural way a ring isomorphism:

$$(3.11) \quad \phi_N : M_N(\mathbb{Z}_m) \xrightarrow{\simeq} M_N(\mathbb{Z}_{p_1^{r_1}}) \oplus \cdots \oplus M_N(\mathbb{Z}_{p_s^{r_s}}).$$

The restriction of  $\phi_N$  on  $\mathrm{GL}_N(\mathbb{Z}_m)$  induces a group isomorphism:

$$(3.12) \quad \phi_N : \mathrm{GL}_N(\mathbb{Z}_m) \xrightarrow{\simeq} \mathrm{GL}_N(\mathbb{Z}_{p_1^{r_1}}) \oplus \cdots \oplus \mathrm{GL}_N(\mathbb{Z}_{p_s^{r_s}}).$$

Obviously, we have

$$(3.13) \quad (\phi_N)_*(\mathcal{U}_N(m)) = \mathcal{U}_N(p_1^{r_1}) \otimes \cdots \otimes \mathcal{U}_N(p_s^{r_s})$$

and

$$(3.14) \quad (\phi_N)_*(\mu_N(m)) = \mu_N(p_1^{r_1}) \otimes \cdots \otimes \mu_N(p_s^{r_s}).$$

In particular, if  $X^{(N)}(p_1^{r_1}), \dots, X^{(N)}(p_s^{r_s})$  are independent Haar random matrices in  $\mathrm{GL}_N(\mathbb{Z}_{p_1^{r_1}}), \dots, \mathrm{GL}_N(\mathbb{Z}_{p_s^{r_s}})$  respectively, then the random matrix

$$\phi_N^{-1}(X^{(N)}(p_1^{r_1}) \oplus \cdots \oplus X^{(N)}(p_s^{r_s}))$$

is a Haar random matrix in  $\mathrm{GL}_N(\mathbb{Z}_m)$ . Moreover, we have

$$\phi_N^{-1}(X^{(N)}(p_1^{r_1}) \oplus \cdots \oplus X^{(N)}(p_s^{r_s}))[S] = \phi_S^{-1}(X^{(N)}(p_1^{r_1})[S] \oplus \cdots \oplus X^{(N)}(p_s^{r_s})[S]).$$

Hence  $X^{(N)}(m)[S]$  and  $\phi_S^{-1}(X^{(N)}(p_1^{r_1})[S] \oplus \cdots \oplus X^{(N)}(p_s^{r_s})[S])$  are identically distributed. By the previous result, we know that for any

$i = 1, \dots, s$ , the law of  $X^{(N)}(p_i^{r_i})[S]$  converges weakly to the uniform distribution  $\mathcal{U}_S(p_i^{r_i})$  on  $M_S(\mathbb{Z}_{p_i^{r_i}})$ . It follows that the law of  $X^{(N)}(m)[S]$  converges weakly to

$$(\phi_S^{-1})_*(\mathcal{U}_S(p_1^{r_1}) \otimes \dots \otimes \mathcal{U}_S(p_s^{r_s})) = \mathcal{U}_S(m).$$

We thus complete the proof of Theorem 3.1.

#### 4. A GENERALIZATION

Let  $\mathbb{F}_q$  denote the finite field with cardinality  $q = p^n$ . Consider the Haar random matrix  $Z^{(N)}$  in  $\mathrm{GL}_N(\mathbb{F}_q)$ . Then we have

**Theorem 4.1.** *The probability distribution  $\mathcal{L}(Z^{(N)}[S])$  of the truncated random matrix  $Z^{(N)}[S]$  converges weakly, as  $N$  tends to infinity, to the uniform distribution on  $M_S(\mathbb{F}_q)$ .*

*Proof.* By combinatoric arguments, we have a similar estimate as (3.9) and the proof of Theorem 4.1 then follows immediately. Here we omit the details.  $\square$

Let  $(\mathcal{A}, +, \cdot)$  be a topological commutative ring with identity which is compact, thus by assumption, the two operations  $+, \cdot : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$  are both continuous. Assume also that  $\mathcal{A}$  is a local ring. Recall that by local ring, we mean that  $\mathcal{A}$  admits a unique maximal ideal. Let us denote the maximal ideal of  $\mathcal{A}$  by  $\mathfrak{m}$ . If we denote by  $\mathcal{A}^\times$  the multiplicative group of the  $\mathcal{A}$ , then we have  $\mathfrak{m} = \mathcal{A} \setminus \mathcal{A}^\times$ . Moreover, let us assume that  $\mathfrak{m}$  is closed.

**Remark 4.1.** *If  $m = p_1^{r_1} \dots p_s^{r_s}$  with  $s \geq 2$ , then the ring  $\mathbb{Z}_m$  is not local. Thus the results in §3 is not a particular case of Theorem 4.5.*

Denote by  $\nu_{\mathcal{A}}$  the normalized Haar measure on the compact additive group  $(\mathcal{A}, +)$ .

**Lemma 4.2** ([5, Lemma 3]). *The quotient ring  $\mathcal{A}/\mathfrak{m}$  is a finite field.*

As a consequence, there exists a positive integer  $q = p^n$  with  $p$  a prime number and  $n$  a positive integer, such that  $|\mathcal{A}/\mathfrak{m}| = q$  and  $\mathcal{A}/\mathfrak{m} \simeq \mathbb{F}_q$ . Let  $\{a_i : i = 0, \dots, q-1\}$  be a subset of  $\mathcal{A}$  which forms a complete set of representatives of  $\mathcal{A}/\mathfrak{m}$ , assume moreover that  $a_0 = 0 \in \mathcal{A}$ .

From now on, as a set, we will identify  $\{a_i : i = 0, \dots, q-1\}$  with  $\mathbb{F}_q$ . For instance, under this identification, we may write

$$\mathcal{A} = \bigsqcup_{i=0}^{q-1} (a_i + \mathfrak{m}) = \bigsqcup_{x \in \mathbb{F}_q} (x + \mathfrak{m}),$$

we also identify the following subset of  $M_N(\mathcal{A})$ :

$$(4.15) \quad \left\{ X = (X_{ij})_{1 \leq i, j \leq N} \mid X_{ij} \in \{a_i : 0 \leq i \leq q-1\}, \det X \in \mathcal{A}^\times \right\}$$

with  $\mathrm{GL}_N(\mathbb{F}_q)$ .

Since  $\mathcal{A}^\times$  is closed, indeed, the group of invertible matrices over  $\mathcal{A}$ :

$$\mathrm{GL}_N(\mathcal{A}) = \left\{ A \in M_N(\mathcal{A}) \mid \det A \in \mathcal{A}^\times \right\},$$

as a closed subset of  $M_N(\mathcal{A})$ , is compact. As a consequence, we may speak of Haar random matrix in  $\mathrm{GL}_N(\mathcal{A})$ , let  $Y^{(N)}$  be such a random matrix. We would like to study the asymptotic law of the truncated random matrix  $Y^{(N)}[S]$  as  $N$  goes to infinity.

**Lemma 4.3.** *We have*

$$(4.16) \quad \mathrm{GL}_N(\mathcal{A}) = \bigsqcup_{X \in \mathrm{GL}_N(\mathbb{F}_q)} (X + M_N(\mathfrak{m})),$$

where we identify  $\mathrm{GL}_N(\mathbb{F}_q)$  with the set given by (4.15).

*Proof.* It is easy to see that for any  $X \in \mathrm{GL}_N(\mathbb{F}_q)$  and any  $X' \in M_N(\mathfrak{m})$ , we have

$$\det(X + X') \equiv \det X \pmod{\mathfrak{m}},$$

hence  $\det(X + X') \in \mathcal{A}^\times$ . This implies that the set on the right hand side of (4.16) is contained in  $\mathrm{GL}_N(\mathcal{A})$ . Conversely, an element  $A \in \mathrm{GL}_N(\mathcal{A}) \subset M_N(\mathcal{A})$  corresponds naturally to a matrix  $X_A \in M_N(\mathcal{A})$  all of whose coefficients are in  $\mathbb{F}_q$  (identified with  $\{a_i : 0 \leq i \leq q-1\}$ ) such that

$$A \equiv X_A \pmod{\mathfrak{m}} \quad \text{and} \quad \det A \equiv \det X_A \pmod{\mathfrak{m}}.$$

As a consequence,  $\det X_A \in \mathcal{A}^\times$  and hence  $X_A \in \mathrm{GL}_N(\mathbb{F}_q)$ . This shows that  $\mathrm{GL}_N(\mathcal{A})$  is contained in the set on the right hand side of (4.16).

Finally, by the definition of the set  $\mathrm{GL}_N(\mathbb{F}_q)$  in (4.16), it is clear that all the subsets  $X + M_N(\mathfrak{m})$ ,  $X \in \mathrm{GL}_N(\mathbb{F}_q)$  are disjoint.  $\square$

As an immediate consequence of Lemma 4.3, we have the following corollary. First recall that we have identified  $\mathrm{GL}_N(\mathbb{F}_q)$  with the set (4.15), hence the random matrix  $Z^{(N)}$  may be considered as a random matrix sampled uniformly from the set (4.15). Note that  $M_N(\mathfrak{m}) \simeq \mathfrak{m}^{N \times N}$  is equipped with the uniform probability

$$(4.17) \quad (q^{-1} \nu_{\mathcal{A}}|_{\mathfrak{m}})^{\otimes (N \times N)}.$$

**Corollary 4.4.** *Assume that we are given a random matrix  $U^{(N)}$  sampled uniformly from  $M_N(\mathfrak{m})$ , which is independent from the random matrix  $Z^{(N)}$ . The random matrix*

$$Z^{(N)} + U^{(N)}$$

*is a Haar random matrix in  $\mathrm{GL}_N(\mathcal{A})$ .*

Note that the distributions of the two random matrices  $U^{(S)}$  and  $U^{(N)}[S]$  coincide.

**Theorem 4.5.** *The probability distribution  $\mathcal{L}(Y^{(N)}[S])$  of the truncated random matrix  $Y^{(N)}[S]$  converges weakly, as  $N$  tends to infinity, to the uniform distribution  $\nu_{\mathcal{A}}^{\otimes(S \times S)}$  on  $M_S(\mathcal{A})$ .*

*Proof.* By Corollary 4.4, the random matrices  $Y^{(N)}[S]$  and  $Z^{(N)}[S] + U^{(N)}[S]$  are identically distributed. Now by Theorem 4.1, the probability distribution  $\mathcal{L}(Z^{(N)}[S])$  converges weakly, as  $N$  goes to infinity, to the uniform distribution on  $M_S(\mathbb{F}_q)$ , hence the probability distribution  $\mathcal{L}(Y^{(N)}[S]) = \mathcal{L}(Z^{(N)}[S] + U^{(N)}[S])$  converges weakly, as  $N$  goes to infinity, to the probability distribution of the random matrix

$$V^{(S)} + U^{(S)},$$

where  $V^{(S)}$  and  $U^{(S)}$  are independent,  $V^{(S)}$  is sampled uniformly from  $M_S(\mathbb{F}_q)$  and  $U^{(S)}$  is sampled uniformly from  $M_N(\mathfrak{m})$ . We complete the proof of Theorem 4.5 by noting that  $V^{(S)} + U^{(S)}$  is uniformly distributed on  $M_S(\mathcal{A})$ .  $\square$

## REFERENCES

- [1] Zhishan Dong, Tiefeng Jiang, and Danning Li. Circular law and arc law for truncation of random unitary matrix. *J. Math. Phys.*, 53(1):013301, 14, 2012.
- [2] Yan V. Fyodorov and Boris A. Khoruzhenko. A few remarks on colour-flavour transformations, truncations of random unitary matrices, Berezin reproducing kernels and Selberg-type integrals. *J. Phys. A*, 40(4):669–699, 2007.
- [3] Christopher J. Hillar and Darren L. Rhea. Automorphisms of finite abelian groups. *Amer. Math. Monthly*, 114(10):917–923, 2007.
- [4] J. Novak. Truncations of random unitary matrices and Young tableaux. *Electron. J. Combin.*, 14(1):Research Paper 21, 12, 2007.
- [5] Seth Warner. Compact noetherian rings. *Math. Ann.*, 141:161–170, 1960.
- [6] Karol Życzkowski and Hans-Jürgen Sommers. Truncations of random unitary matrices. *J. Phys. A*, 33(10):2045–2057, 2000.

YANQI QIU: CNRS, INSTITUT DE MATHÉMATIQUES DE TOULOUSE, UNIVERSITÉ PAUL SABATIER, 118 ROUTE DE NARBONNE, F-31062 TOULOUSE CEDEX 9, FRANCE

*E-mail address:* yqi.qiu@gmail.com